UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,667	09/30/2003	Germano Caronni	03226/296001; P9007	5817

32615 7590 06/03/2010

OSHA LIANG LLP/Oracle
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
06/03/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
lord@oshaliang.com
hathaway@oshaliang.com

Supplemental Notice of Allowability	Application No.	Applicant(s)	
	10/675,667	CARONNI, GERMANO	
	Examiner	Art Unit	
	FARID HOMAYOUNMEHR	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *applicant's filing dated 2/24/20, interview dated 4/20/10, and Office Action sent 4/30/10* .

2. ☒ The allowed claim(s) is/are *1-7, 13-23 now renumbered as 1-18,*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Farid Homayounmehr/ Examiner Art Unit: 2439	

DETAILED ACTION

This Supplemental Notice of Allowability is to apply the correct underlining required for amendments to the claims. The only change relative to the Notice of Allowability sent on 4/30/2010 is in the section titled "In the claims", wherein the correct underlining is applied.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Robert Loyd on 4/20/2010.

In the claims:

1. (Currently Amended) A method for re-encrypting encrypted data in a secure storage file system, comprising:

obtaining one or more selected encrypted data blocks from the secure storage file system, each selected encrypted data block comprising a selected encrypted data, the one or more selected encrypted data blocks comprising data blocks accessed by a first user, wherein the one or more selected encrypted data blocks were selected based on ~~using~~ a user data

access record, wherein the user data access record comprises a bitmap indicating which encrypted data blocks [[is]] are accessed by a first user;

decrypting, re-encrypting and storing each one of the one or more selected encrypted data blocks, the decrypting, re-encrypting and storing of each data block comprising:

decrypting the selected encrypted data using a first symmetric key associated with the encrypted data block to obtain selected data;

re-encrypting the selected data using a second symmetric key associated with the data block to obtain new encrypted data;

for each user who has access to the data block,

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

storing in a new data block, stored in a storage device;

the new encrypted data and the new encrypted symmetric key if a second user has read permission, wherein the second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the private key to obtain encrypted hash data; and

storing the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission.

2. (Previously Presented) The method of claim 1, wherein the user data access record comprises at least one selected from the group consisting of a bitmap for each user and a bitmap for each group of users.

3. (Original) The method of claim 1, wherein the write permission comprises at least one sub-division.

4. (Original) The method of claim 3, wherein the sub-division is selected from a group consisting of insert, append, truncate, and delete.

5. (Original) The method of claim 1, wherein the secure storage file system is implemented using a preloaded shared library.

6. (Original) The method of claim 5, wherein the preloaded shared library translates read/write/file name accesses into different read/write/file name accesses.

7. (Original) The method of claim 1, wherein the secure storage file system is implemented using a shared library that includes functionality to map read/write/file name accesses to a custom-implemented file system.

8.–12. (Canceled)

13. (Currently Amended) A computer system generating a secure storage file system, comprising:

a processor;

a memory;

a storage device;

a computer display; and

software instructions stored in the memory for enabling the computer system under control of the processor, to perform:

obtaining one or more selected encrypted data blocks from the secure storage file system, ~~using a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user~~ each selected encrypted data block comprising a selected encrypted data, the one or more selected encrypted data blocks comprising data blocks accessed

by a first user, wherein the one or more selected encrypted data blocks were selected based on a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data blocks are accessed by a first user;

decrypting, re-encrypting and storing each one of the one or more selected encrypted data blocks, the decrypting, re-encrypting and storing of each data block comprising:

decrypting the selected encrypted data using a first symmetric key associated with the data block to obtain selected data;

re-encrypting the selected data using a second symmetric key associated with the data block to obtain new encrypted data;

for each user who has access to the data block,

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

storing in a new data block, stored in a storage device the new encrypted data and the new encrypted symmetric key if a second user has read permission, wherein the second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the public key to obtain encrypted hash data; and

storing the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission.

14. (Original) The computer system of claim 13, wherein the write permission comprises at least one sub-division.

15. (Previously Presented) The computer system of claim 14, wherein the sub-division is selected from a group consisting of insert, append, truncate, and delete.

16. (Original) The computer system of claim 13, wherein the secure storage file system is implemented using a preloaded shared library.

17. (Original) The computer system of claim 16, wherein the preloaded shared library translates read/write/file name accesses into different read/write/file name accesses.

18. (Original) The computer system of claim 13, wherein the secure storage file system is implemented using a shared library that includes functionality to map read/write/file name accesses to a custom-implemented file system.

19. (Previously Presented) The computer system of claim 13, wherein the user data access record comprises at least one selected from the group consisting of a bitmap for each user and a bitmap for each group of users.

20. (Currently Amended) A secure storage system comprising:

a storage provider storing encrypted data in a storage device, ~~wherein re-encrypting the encrypted data comprises:~~

obtaining one or more selected encrypted data blocks from the secure storage file system, each selected encrypted data block comprising a selected encrypted data, the secure storage file system executing on the storage provider using a user data access record in response to receiving a key re-encryption event, ~~wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;~~

~~decrypting the selected encrypted data using a first symmetric key to obtain selected data;~~

the one or more selected encrypted data blocks comprising data blocks accessed by a first user, wherein the one or more selected

encrypted data blocks were selected based on a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data blocks are accessed by a first user;

decrypting, re-encrypting and storing each one of the one or more selected encrypted data blocks, the decrypting, re-encrypting and storing of each data block comprising:

decrypting the selected encrypted data using a first symmetric key associated with the encrypted data block to obtain selected data;

re-encrypting the selected data using a second symmetric key associated with the data block to obtain new encrypted data;

for each user who has access to the data block,

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

storing in a new data block, stored in the storage device, the new encrypted data and the new encrypted symmetric key if a second user has read permission, wherein the second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the private key to obtain encrypted hash data; and

storing the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission; and

a client device, wherein the client device comprises a client kernel for generating the key re-encryption event and a client application using the encrypted data.

21. (Previously Presented) The system of claim 20, wherein the user data access record comprises at least one selected from the group consisting of a bitmap for each user and a bitmap for each group of users.

22. (Original) The system of claim 20, wherein the write permission comprises at least one sub-division.

23. (Original) The system of claim 22, wherein the sub-division is selected from a group consisting of append, truncate, and delete.

24.– 30. (Canceled)

Response to Arguments

6. Applicant's argument relative to the rejections under section 112 in light of the amendments made in their response filed 2/24/2010 has been found persuasive. The rejections are hereby withdrawn.

Applicant's argument relative to prior art rejection in light of the amendments noted by this action, and the telephone interview conducted on 4/20/2010 have been found persuasive (please see the attached Interview Summary).

Allowable Subject Matter

7. Amended claims 1-7, 13-23 now re-numbered as claims 1-18 are allowed.

Examiner's Statement of Reasons for Allowance

8. The following is an examiner's statement of reasons for allowance:

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed, particularly the feature of selecting data accessed by a user based on a bit map access record, decrypting all accessed data, and re-encrypting all the accessed data with a new symmetric key and encrypting the symmetric key using the public key of each system user separately, and saving the encrypted symmetric keys encrypted using the public keys of each user in a separate data block along with the encrypted data, and depending on each user's read/write permission, also storing a hash of the accessed data in each data block, among other features of the independent claims.

Conclusion

9. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Farid Homayounmehr/
Examiner
Art Unit 2439